UNITED STATES MARINE CORPS
MARINE CORPS LOGISTICS BASES
814 RADFORD BOULEVARD
ALBANY, GEORGIA 31704-0323

IN REPLY REFER TO:
2000
G600

DEC 17 2001

POLICY STATEMENT 4–01

From: Commander
To: Distribution List

Subj: AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY POLICY

Ref: (a) SECNAVINST 5239.3 DON INFOSEC Program
(b) MCO 5500.13A, Physical Security
(c) SECNAVINST 5510.30A, Department of the Navy Personal Security Program
(d) IRM 5239-10 Small Computer Systems Security
(e) MARADMIN 162/00, Appropriate use of Government Information Technology Resources
(f) MARADMIN 541/99 Use of Commercial Electronic Mail Services
(g) SECNAVINST 5720.47, DON Policy for Content of Publicly Accessible WWW Sites
(h) Marine Corps Order 5720.26, Standardization of Publicly Accessible Web Pages
(i) MARADMIN 140/01, Electronic and Information Technology Accessibility Standards
(j) IRM 5239-09 Contingency Planning
(k) OPNAVINST 2201.2, Navy and Marine Corps Computer Network Incident Response
(l) NAVSO Pub 5239-19 Computer Incidence Response Guidebook
(m) MARADMIN 158/98, Information Assurance Training and Certification (IAT&C)
(n) IRM 5239-08A, Computer Security Procedures

Encl: (1) MARCORLOGBASES Acceptable Computer Use Agreement Form

1. Purpose. The purpose of this policy is to define the Information Security (INFOSEC) guidelines that will ensure the confidentiality, integrity, availability, non-repudiation, and authentication of all Marine Corps Logistics Bases (MARCORLOGBASES) AIS. This policy ensures all actions are taken to comply with the instructions provided in reference (a).

2. Definition. An AIS is defined as any equipment, interconnected system, or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Peripherals, hardware, software, firmware, and all information services are included. Violations of this policy may result in administrative, disciplinary, or legal actions. All references apply.

3. Responsibilities.

a. The Assistant Chief of Staff, Information Technology Department (G6) has been assigned as the Designated Approving Authority (DAA) for MARCORLOGBASES. The DAA is ultimately responsible for all Information Assurance (IA) security matters within the Command. The DAA will ensure user compliance with these security directives.

b. The MARCORLOGBASES G6 Information Systems Security Manager (ISSM) is appointed by the DAA as the designated representative of the MARCORLOGBASES Commander for all IA security and will have direct access to the MARCORLOGBASES Commander on matters of IA security. The G6 ISSM will act as the focal point for all Information Systems Security matters. The G6 ISSM is responsible for planning, developing, and implementing a comprehensive IA security program for MARCORLOGBASES. The G6 ISSM will ensure that personnel comply with all MARCORLOGBASES IA security instructions and related DoD directives.

c. Each Base Commander will appoint, in writing, one Base Level DAA for their Command. The Base Level DAA is the Base Commander's designated representative responsible for ensuring that the MARCORLOGBASES IA program is implemented at their local Command and for ensuring that the required Certification and Accreditation processes are completed for local systems and local site networks.

d. Each Base Commander will appoint, in writing, one Base Level ISSM for their Command. The Base Level ISSM is the Base Commander’s designated representative responsible for ensuring that all security measures at their Command are implemented according to MARCORLOGBASES policy. The Base Level ISSM will have direct access to the MARCORLOGBASES G6 ISSM for all IA matters.

e. Information Systems Security Officers (ISSOs) are the designated representatives responsible for implementing, maintaining, and administering the comprehensive IA security program for each AIS under their control. The ISSOs will have direct access to the Base Level ISSMs for all IA Security matters. The Directors of the local Information Technology (IT) support sections, i.e., S6/ISO/ISMO, will appoint ISSOs in writing. The number of ISSOs will depend on the workload and number of systems under their operational control.

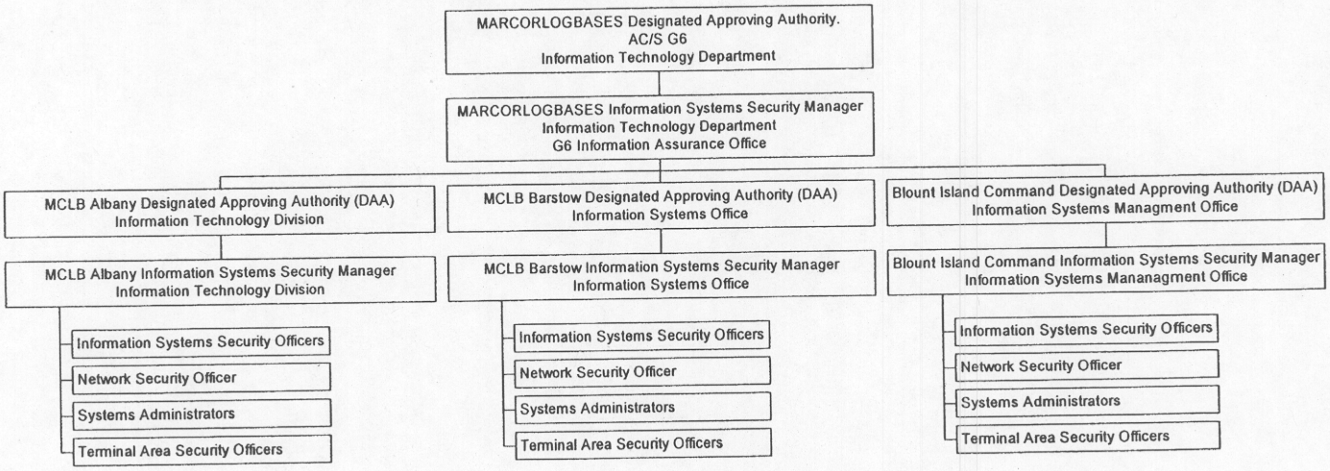
f. Network Security Officers (NSOs) will oversee the processing of classified and sensitive unclassified data for each Local Area Network. The Director of the local IT support sections will appoint an NSO in writing. NSOs will ensure that standard security procedures and measures that support the security of the entire network are implemented to include all network components and services.

g. System Administrators (SAs), who are responsible for the administration and operation of an IS, work with the ISSO to ensure that the IS operates in accordance with Command security policies and procedures. SAs will provide technical expertise and assistance to the ISSOs and NSOs as required. The SA may also be the ISSO or NSO for his or her particular IS(s) or network.

h. Terminal Area Security Officers (TASOs) provide, in conjunction with the Base Level ISSM, the ISSO, and the NSO, specific guidance to all users and operating personnel with respect to the secure operation of IT resources in their designated areas. Each Division will appoint in writing a TASO to provide security awareness for their designated areas. TASOs can be the same individual as the Information Systems Coordinator (ISC).

i. Organizational structure diagram.

MARCORLOGBASES INFORMATION ASSURANCE ORGANIZATIONAL STRUCTURE


MARCORLOGBASES Designated Approving Authority.
AC/S G6
Information Technology Department
MARCORLOGBASES Information Systems Security Manager
Information Technology Department
G6 Information Assurance Office
MCLB Albany Designated Approving Authority (DAA)
Information Technology Division
MCLB Barstow Designated Approving Authority (DAA)
Information Systems Office
Blount Island Command Designated Approving Authority (DAA)
Information Systems Managment Office
MCLB Albany Information Systems Security Manager
Information Technology Division
MCLB Barstow Information Systems Security Manager
Information Systems Office
Blount Island Command Information Systems Security Manager
Information Systems Mananagment Office
Information Systems Security Officers
Network Security Officer
Systems Administrators
Terminal Area Security Officers
Information Systems Security Officers
Network Security Officer
Systems Administrators
Terminal Area Security Officers
Information Systems Security Officers
Network Security Officer
Systems Administrators
Terminal Area Security Officers

4. <u>Compliance</u>. All MARCORLOGBASES personnel will familiarize themselves with this document and its references and ensure strict compliance. Criminal violations of this policy will be documented and turned over to the proper investigative authorities by the G6 ISSM and may result in disciplinary action under the UCMJ or civil prosecution. The MARCORLOGBASES G6 ISSM, with the assistance of the Base Level DAAs, Base Level ISSMs, ISSOs, NSOs, SAs and TASOs, will monitor and report all violations of this policy to the MARCORLOGBASES DAA.

5. Policy Areas.

a. Physical Security. All IT equipment will be properly marked and accounted for per reference (b). Personnel working in buildings containing AIS assets will secure all doors and windows at the close of business each day or when the building will be unattended for any extended length of time. Any questions or problems concerning physical security of IT will be directed to the designated Base ISSM or Base Security Manager. The Base ISSM, Base Security Manager and the Provost Marshal are responsible for physical security measures as necessary to prevent accidental or malicious damage to hardware, software, data or furnishings; exposure of sensitive or classified data to unauthorized personnel; theft or unauthorized removal of hardware, software or data; and/or access by persons intent upon terrorist, destructive, or other criminal acts.

b. Personnel Security. Per reference (c), a National Agency Check with written Inquiries (NACI) or better will be conducted on all Government Service personnel as they are processed for initial employment. Personnel having access to classified information will be given a command security orientation outlining the proper actions required to process and handle classified information and will receive annual refresher briefings. Only authorized users will be allowed access to an AIS covered by this policy.

c. Small Systems Security. Due to the large number of Personal Computers (PC) that are spread throughout the command, the security for these systems and the data they contain falls heavily upon the user. It is the responsibility of the individual user to safeguard the information stored on these computers. The protection of information processed on the Command's information resources will be handled in accordance with reference (d). Additionally, local IT support sections will ensure all Network and System Administrators use effective and secure processes in maintaining networks and systems. Local IT support sections will develop written secure Standard Operating Procedures for administrator use.

d. Software Security. The Marine Corps honors all licenses, copyrights, patents, restrictions, and terms and conditions associated with commercial, proprietary computer software. Detailed guidance and procedures for software security will be published in a future policy statement.

e. Internet Security. Gaining Access to the World Wide Web will be done through authorized Marine Corps channels only. Users will adhere to the guidelines spelled out in reference (e). Procedures will be implemented at each Local Command to monitor Internet traffic and to restrict access to unauthorized web sites. Detailed guidance and procedures for Internet use will be published in a future policy statement.

f. Electronic Mail. E-mail has become an integral part of conducting daily business throughout the Marine Corps. All personnel using the MCEN for Email will adhere to the regulations governing the proper use of Electronic Mail as set forth in references (e) and (f). Detailed guidance for proper Email use will be published in a future policy statement.

g. Web Page Security. All information posted will adhere to the guidelines set forth in reference (g), (h), and (i). Detailed guidance for web page posting will be published in a future policy statement.

h. Contingency Planning. Contingency plans for each information system and/or network will be developed and maintained in accordance with reference (j) and will be incorporated into the Command Contingency Plan.

i. Virus Protection. All MARCORLOGBASES AIS and communication networks are targets for attacks. Users, maintainers, and administrators must be vigilant about preventing viruses from infecting information systems and networks. Whenever possible, SAs should implement the updates to software and signature files via an automated process. At a minimum, the following virus protection actions will be performed to prevent widespread infection of malicious code:

(1) Marine Corps approved virus protection software will be installed on all ISs within the command and the virus signature files updated whenever a new virus signature list is released by the anti-virus software manufacturer.

(2) All media (floppy disk, hard disk, CD-ROM, tape, etc.) and files (E-mail attachments, documents from web sites, etc.) will be scanned with virus protection software prior to their initial use on an IS.

(3) All ISs will be scanned at least weekly with virus protection software.

j. Incident Reporting. The term "incident" refers to an adverse event in an IS and/or network, or the threat of occurrence of such an event. Per reference (k), written procedures shall be established and maintained that will enable a rapid response to an incident, or threat of an incident. Reference (l) is also an additional source for establishing local computer incident response procedures. Detailed guidance for computer incident response will be published in a future policy statement.

k. Information Assurance Awareness Training. It is imperative that all individuals using, administering, and maintaining ISs understand the threats to these systems and the policies, procedures, and equipment designed to mitigate these threats. Per reference (m), all SAs, users, and maintainers of AIS will receive the appropriate security certification training. A detailed program for IAT&C will be published in a future policy statement.

l. Sensitive Information Handling. Data will be safeguarded per references (d) and (n) to provide a secure environment for data both stored and processed. Data can be stored on diskettes, tapes, CDs, zip disks, other backup media, AIS and printed material. The use, backup, accessibility, maintenance, movement, and disposition of data will be controlled on the basis of its level of classification, location of use, type of data, and personnel "need to know". Materials, AIS generated documents, and all AIS storage media will display appropriate security markings.

m. Configuration Management. Hardware and software configuration controls are critical throughout the life cycle of AIS as changes to these components may have potential security implications. AIS security will be a consideration in all decisions concerning changes to hardware and software components, to include changes to the local area network (LAN). Guidance for configuration management will be published in a future policy statement.

n. Third Party Network Connection. Local Commands will develop processes to ensure a secure method of network connectivity for third-party companies and provide a formalized method for the request, approval, and tracking of such connections. Detailed guidance for third-party network connection will be published in a future policy statement.

o. New Account Creation. All new personnel, to include on-site contractors, will read, understand, and sign enclosure (1), prior to being issued an account and password. Personnel already employed by MARCORLOGBASES, to include on-site contractors, will be required to read, understand, and sign the MARCORLOGBASES Acceptable Computer Use Agreement Form and its enclosures. Failure to read and sign the form will result in their account being disabled until the signed document is turned into their local computer security section. The Base Level ISSM will keep all signed computer use agreement forms on file.

p. Passwords. Passwords will be used to limit access to MARCORLOGBASES AIS resources. Local IT support sections will use automated procedures to help enforce written password security policies. Detailed guidance to assist End Users in password use will be published in a future policy statement.

6. Administrative Actions. Failure to abide by this policy will result in administrative or punitive action. This may include loss of account access.

7. Point of Contact. Address questions concerning Information Assurance to MARCORLOGBASES AC/S, Information Technology Department, Information Assurance Office (G620) at DSN 567-7133 or Commercial (229)-639-7133. Email is matcomg6iaoffice@matcom.usmc.mil. Information can also be obtained from the MARCORLOGBASES G6 Information Assurance Office website at http://www.ala.usmc.mil/iao.

8. Applicability. This policy is applicable throughout all activities aboard MCLB Albany, MCLB Barstow, and Blount Island Command. This document also applies to all AIS, classified and unclassified, used by military, civilian and contractor personnel under MARCORLOGBASES.

R.S. Kramlich
R. S. KRAMLICH

Distribution: A

MARCORLOGBASES ACCEPTABLE COMPUTER USE AGREEMENT FORM

1. By my signature, I certify that I have read and understood: 1) this document, 2) the latest version of the Marine Corps Logistics Bases (MARCORLOGBASES) Internet Use Policy, and 3) the latest version of the MARCORLOGBASES Use of Electronic Mail (Email) Services Policy, and agree to the terms identified in this document. Failure to do so will result in denial of access to MARCORLOGBASES Automated Information System (AIS) resources. If I have questions relative to AIS security at any time during my employment, it is my responsibility to contact the Information Systems Security Manager (ISSM) or the Information Systems Security Officer (ISSO).

2. I understand the resources I am using are United States Marine Corps (USMC) computer systems. These computer systems, including all related equipment, networks and network devices (specifically including internet access), are provided only for AUTHORIZED U.S. GOVERNMENT USE.

3. I understand that USMC Computer systems will be MONITORED for all lawful purposes, including AUTHORIZED USE, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

4. I understand use of a USMC computer system, authorized or unauthorized, constitutes consent to monitoring of the system. Unauthorized use may subject the user to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action.

5. I will not process or store classified information on AIS resources not specifically approved for this purpose and will report all inadvertent/unapproved classified processing to the ISSM immediately so that the system(s) may be sanitized. If the ISSM/ISSO are not available, I will contact the local Communication Security Material Systems (CMS) Custodian.

6. I will not copy (other than for backup), modify, or transfer Government/Marine Corps purchased computer programs unless granted by the license of that product, and will only use software on the AIS resources for which they are intended. I understand making unauthorized copies of software is a violation of copyright laws, and employees are subject to indictment and conviction under military, civil and/or criminal law if found guilty.

7. I will protect passwords from unauthorized access and will not share them with co-workers or other personnel. I will change passwords at least every 90 days or as required by the system administrators. If I feel that my password has been compromised, I will change it immediately.

8. I will not remove AIS resources from MARCORLOGBASES workspaces without notifying my Responsible Officer and receiving express written permission from the computer section.

9. I will promptly report all loss, theft, damage, suspicion of intrusion, malicious code (virus), and/or compromise of any AIS resources to the ISSM.

10. I will not bring personally owned AIS resources, either hardware or software, for use on government-owned Information Technology resources.

11. I will not load or use entertainment software on any AIS resource belonging to the United States government.

12. I will not load or use any shareware/freeware software on any MARCORLOGBASES-owned AIS resource.

13. I understand misuse of the Internet may result in administrative or punitive action and, if warranted, criminal prosecution.

14. I understand that accessing Commercial Email services from USMC owned resources is forbidden.

15. I understand that failure to comply with the policies set forth in this document will result in administrative or punitive action. This action may include loss of account access. This document does not relieve me from complying with other regulations as given in various documents.

NAME (Print)	Est. Date of Departure/Expiration Date
Mother's Maiden Name	County Born In
SIGNATURE	DATE